Towards Purpose Enforcement Model for Privacy-aware Usage Control Policy in Distributed Healthcare

Rath, Thavy Mony Annanda; Colin, Jean-Noël

Published in:
International Journal of Security and Networks

Publication date:
2013

Document Version
Early version, also known as pre-print

Towards purpose enforcement model for privacy-aware usage control policy in distributed healthcare

Annanda Thavymony Rath* and Jean-Noël Colin

PReCISE Research Center,
Faculty of Computer Science,
University of Namur,
rue de Bruxelles 61, B-5000 Namur, Belgium
Email: rath.thavymony@unamur.be
Email: jean-noel.colin@unamur.be
*Corresponding author

Abstract: Enforcing the purpose of data usage means to ensure that data are used as it intends for and that excessive usage cannot happen. In general, the enforcement of purpose is a complicated task. The main difficulty is to identify the purpose of an agent when it requests to perform an action. In this paper, we discuss the design issue of usage purpose enforcement model based on our proposed enforcement structure: pre-, ongoing-, and post-enforcement. We also propose an enforcement solution for usage control designed for distributed healthcare information system, particularly, the pre- and ongoing-enforcement of purpose. Furthermore, we validate our model with a prototype developed in Java.

Keywords: purpose enforcement; enforcement model; distributed healthcare; security; privacy.

Reference to this paper should be made as follows: Rath, A.T. and Colin, J-N. (2013) 'Towards purpose enforcement model for privacy-aware usage control policy in distributed healthcare', *Int. J. Security and Networks*, Vol. 8, No. 2, pp.94–105.

Biographical notes: Annanda Thavymony Rath is currently a PhD student in Faculty of Computer Science, University of Namur, Belgium. He received Computer Science Engineering degree in 2004 from Cambodia Institute of Technology and Master of Computer Science degree in 2006 from Indian Institute of Technology Bombay, India. His research focuses on data and application security, particularly, access control, usage control, rights management and enforcement in an open environment.

Jean-Noël Colin is Professor at the Computer Science Faculty of University of Namur, Belgium, and a permanent member of the PReCISE Research Center. His teaching and research activity are information systems security, and in particular, authentication and authorisation protocols, rights management and access and usage control in privacy-sensitive environments.

1 Introduction

Over the last decade, with the increase of electronic materials in healthcare and the improvement of network and information system, 'electronic health records' have become increasingly common and widespread to replace the traditional paper based-record (Lillian, 2008; Rengamani et al., 2010). However, making the information available electronically poses new security concerns especially when sharing them between different healthcare institutions where control of usage is required. Health records are important in the course of treatment process for the proper continuing care for patient and in most countries, they are considered as sensitive private data and they require special protection when using them.

For example, the privacy legislations in Europe, USA or Canada clearly mention that 'health records' are considered as sensitive private data and their processing are bounded to the specific 'purpose' and excessive use of them is prohibited. With this regard, any processing environment dealing with such data requires great attention to make sure that system can provide adequate data processing security aligning with privacy legislation. The need of limiting the usage of data within the allowed 'purpose' leads to the need of effective management of purpose binding of data (including the recognition of purpose binding data) and enforcement. In general, there are two main parts for purpose enforcement.

1 First, 'verification', a process to prove that claimed purpose exists for given requested object and action.

2 Second, 'validation' refers to a process to prove that the claimed purpose is valid at the time of usage. For example, if physician claims 'heart-surgery' as purpose of using patient health record, then, 'validation' means to prove that physician does have the right to use data

for 'heart-surgery', requested purpose can be achieved after usage permission is granted, and physician cannot use patient's record beyond the authorised purpose.

Validating purpose of action is the main difficulty in purpose enforcement. Some common proposed mechanisms for purpose management and enforcement are: self-declaration, in which the agent explicitly announces the purpose of data usage (Byun et al., 2005), and role-based enforcement (Jawad et al., 2008b), in which the purpose is identified based on the agent's role in the system. The first method obviously cannot stop malicious agent from claiming false purposes. This is because anyone can claim any purpose of usage, without the proper system to validate claimed purpose; this method cannot be used in data processing environment like distributed healthcare (Rath and Colin, 2012a; Rath and Colin, 2012b; Jafari et al., 2011). The second method has been criticised to be inefficient in capturing the purpose of an action since roles and purposes are not always aligned and members of the same organisational role may practice different purposes in their actions. Therefore, validating the claimed purpose remains an open question.

This paper addresses three main issues: (a) propose purpose enforcement structure, (b) propose the design of purpose validation for the three validation phases (pre-, ongoing-, and post-enforcement) for distributed healthcare; and (c) implement the proposed model in a Java program, as the validation for our proposed model. It is worth noting that in this paper, we focus on usage control, more importantly, the enforcement of privacy-aware usage policy. In order to make a clear distinction between access and usage control, we provide the brief definitions as following.

- Access control (Ferraiolo et al., 2001) is to selectively determine who can access services or resources and what type of permission is provided exactly. Access control prevents unauthorised access to the resources of system and they are implemented as a result of certain access control requirements, which are generally in line with the institutions policies.
- Usage control (Alexander et al., 2008) refers to what should and should not happen to data item once it is granted access. Usage control is generally a controlling process at client side where data reside after usage permission is granted. When users request data from data provider, they might have to commit themselves to an access and usage control policy that reflects the data provider or owner's interest. In general, access policy is applied at the time when users initiate request to data at server side and usage policy is applied at client when users start to process data at client-side control domain (Alexander et al., 2006).

The dedicated usage control mechanism/technique can give the data owner a sufficient amount of control over what data consumer can do when the data are out of the controlling environment of the server side control domain.

The rest of the paper is organised as follows. Section 2 presents the motivation and related work. Section 3 discuses about the purpose model and its enforcement structure. A purpose enforcement model for usage control is presented in Section 4 and a prototype of the proposed model in Section 5. The discussion on the perspective concerning purpose enforcement and the future research direction is presented in Section 6. Section 7 gives the conclusion.

2 Motivation and related work

Securing the processing of private data in distributed environment has been the subject of intense research, given the rise of social network and e-health systems. Many researches have contributed to this aspect ranging from access control, usage control, usage policy expression languages, secure communication protocol, and enforcement of usage policy (Li and Hoang, 2009; Russello et al., 2008; Lillian, 2008; yarmand et al., 2008). Among them, enforcing the privacy-aware usage policy is the main challenge, given the fact that, in distributed environment, the direct control on data is not possible. Thus, it is hard to ensure that remote client processes data as stipulated in usage policy without proper controlling technique.

Jafari et al. (2011) defined a semantic model for purpose, based on which purpose-based privacy policies can be expressed and enforced in a business system. The model is based on the intuition that the purpose of an action is determined by its position among other inter-related actions. Actions and their relationships can be modelled in the form of an action graph. A modal logic and model checking algorithm are developed for formal expression of purpose-based policies and for verifying whether a particular system complies with them.

Rath and Colin (2013a) defined the access and usage control requirements for a particular healthcare information system where patients have pivotal right to grant or deny access to their health records. Authors named this system 'Patient Controlled Record type of Healthcare Information System or PCRHIS'. They also identified different types of users who are responsible for processing patient's record. Rath and Colin (2013b) also purpose a model for e-health system. They classified purpose in different categories and defined the relationship between them. The usage enforcement engine is also proposed to support the model.

Byun et al. (2005) and Ni et al. (2010) proposed a purpose-based access control model of complex data for privacy protection, a model that relies on the well-known RBAC (Ferraiolo et al., 2001) access control model as well as the notion of conditional role which is based on the concept of role attribute and system attribute. In their paper, they also provided a general purpose tree applied in complex data management system and a solution to address the problem of how to determine the purpose for which certain data are accessed by a given user.

Concerning usage enforcement, Katt et al. (2008) proposed the extension of $UCON_{abc}$ (Park and Sandhu, 2002) with continuous control usage sessions for expressing the ongoing-check obligation. They also proposed the general, continuity-enhanced policy enforcement engine for

usage control applied particularly to obligation. After the thorough study on the work of Katt et al., we found that the model can be extended and used to enforce the ongoing-enforcement of purpose.

Jawad et al. (2008a) proposed the formalised and enforced purpose restrictions in privacy policies based on planning. They modelled planning using a modified version of Markov Decision Processes (MDPs). They argued that an action is for a purpose if and only if the action is part of a plan for optimising the satisfaction of that purpose under the MDP model. Authors used this formalisation to define when a sequence of actions is only or not for a purpose. With this semantics, authors created and implemented an algorithm for auditing it.

Another method is based on workflow like the one proposed by Jafari et al. (2009), Russello et al. (2008) and Zhang et al. (2005); they proposed an approach to enforce purpose using workflows, and encoded purposes as properties of workflows used in organisations. However, the proposed model does not work with 'purpose' that does not have a natural interpretation in terms of workflows, particularly, more abstract purposes.

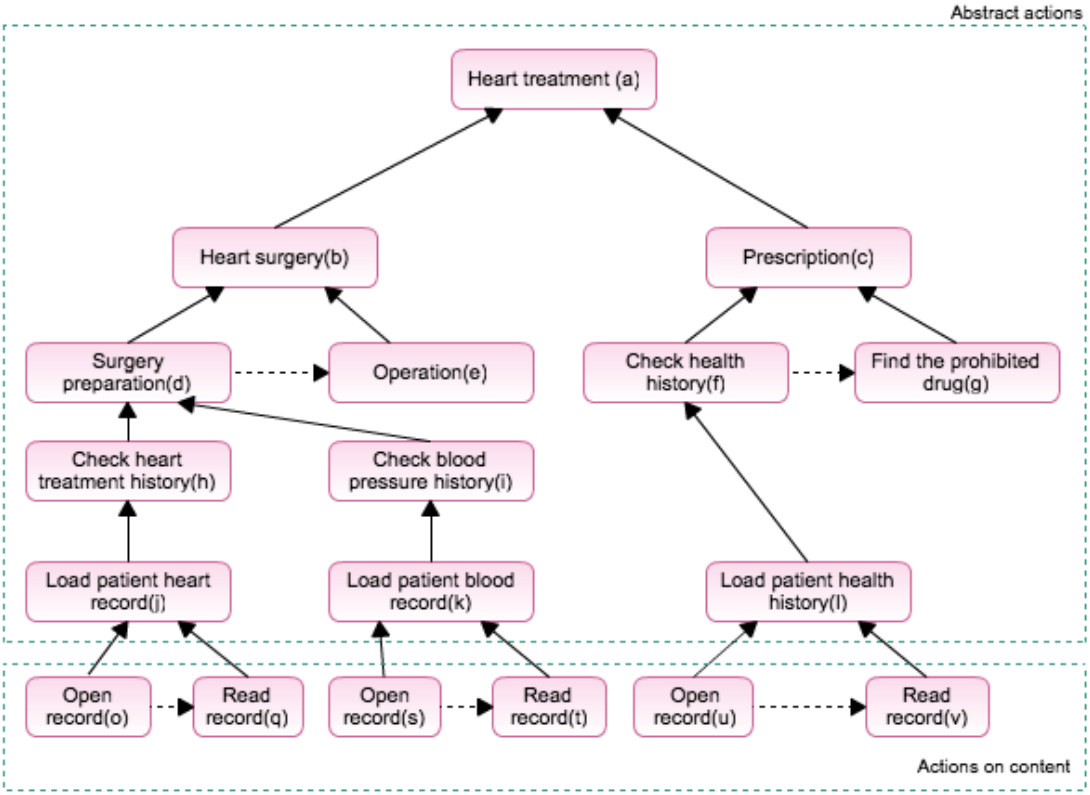
3 Purpose model and its enforcement structure

Purpose of usage is one of the core concepts in privacy which considers user's intent as a factor in making usage control decisions. In dictionary, 'purpose' is defined as 'the object towards which one strives or for which something exists; an aim or a goal'. However, observing how purpose is used in the natural language reveals that purposes often refer to a set of abstract actions. For example, accessing patient's health record for the purpose of treatment, research, insurance, etc., all of which are names of some abstract actions. Jafari et al. (2011) classified 'purpose' in two types: purpose as high-level action and purpose as future action.

Purpose as a high-level action refers to a more abstract or semantically higher level action in a plan. Thus, doing something for some purposes, actually means doing it as a part, or a sub-action, for that higher level action. For example, when Bob checks some patient's blood pressure for the purpose of heart surgery, it means that checking the blood pressure is a part of a more complex and abstract action of heart surgery. As presented in Figure 1, the abstract action 'purpose' (a) is considered as the high-level action of '(b)–(v)'.

Purpose as a future action is used to indicate that an action is performed as a prerequisite of another action in future. For example, in Figure 1, when a doctor does the 'surgery preparation' for a purpose of 'operation', it means the former action 'surgery preparation' is done as a prerequisite to performing the later action which is 'operation'. In Figure 1 '(e)(g)(q)(t)(v)' are considered to be the future action of '(d)(f)(o)(s)(u)', respectively.

Figure 1 Example of purpose graph in healthcare where dashed arrows represent purpose as 'future action' and solid arrows represent 'purpose' as 'high level action'. They are read from bottom up for solid arrows (e.g. 'surgery preparation' is a high-level action of 'check heart treatment history'). Dashed arrows are read from left to right (e.g. 'operation' is a future action of 'surgery preparation') (see online version for colours)



Overall, to enforce the purpose means to verify that those abstract actions exist and they are valid during the usage of data. But the question is when and how the purpose should be enforced during the lifecycle of data usage.

Observing how data are processed in the real world reveals that there are three crucial states that need to be considered for the enforcement of purpose: before usage permission is granted, during the usage of data, and after using it. We name the three enforcement states as: pre-, ongoing-, and post-enforcement.

- Pre-enforcement refers to a mechanism allowing system to validate the purpose before granting usage permission to data. At this stage, the user's request in which the purpose of usage is mentioned is validated by the system. If the system finds that the claimed purpose is not valid, it rejects request immediately without going further into the details evaluation of usage policy. For example, in emergency case for heart-surgery purpose, if doctor declares that purpose and system cannot prove the existence of 'emergency heart-surgery', then the request is rejected.
- Ongoing-enforcement refers to a mechanism allowing system to continuously control purpose of usage during the usage period. It checks if the actions performed and the requesting actions comply with the claimed purpose. During the usage, the system periodically triggers the re-evaluation of purpose. This intends to check if the purpose of usage is still valid given the change of time or state. Ongoing-enforcement can be called 'controlling and guiding method' because it acts as a controller and also a guide for user. It tells the user which action is allowed for which purpose.
- Post-enforcement refers to a mechanism allowing system to validate the processing of data and to identify if the usage of data was in line with the claimed purpose or otherwise. This enforcement is done after the usage of data. It provides a way to prove the correctness of the data usage by means of the log information. Auditing mechanisms are required to analyse the log information and to reconstruct the execution process in order to find out if violation happened or not.

With the above consideration, we see that to ensure the correctness of data usage, the purpose validation in those three states must be maintained. To support this enforcement structure, we propose the purpose validation information model as following. We define purpose as a tuple of PV (Purpose Validation) that consists of four elements as following.

$$PV = F(CP, EP, T, VM)$$

where

- 'CP' is a claimed purpose of data usage.
- 'EP' is an enforcement phase, it tells when the purpose should be checked, it can be 'pre-enforcement, ongoing-enforcement, or post-enforcement'.
- 'T' is used for ongoing-enforcement and post-enforcement. When it is used in ongoing-enforcement, 'T' refers to the time period for re-validating purpose. For example, during the emergency treatment session, re-validating purpose every 30 minutes. In case of post-enforcement, 'T' refers to a time at which the purpose validation takes place after the data usage is ended. For example, re-validating the purpose of usage after two days of data usage.
- 'VM' is validation mechanism which describes the mechanism used to check the validity of claimed purpose.

In general, these four information elements are attached to data and they are sent to the remote client. With the provided information, remote client configures its system and validates purpose accordingly.

For example, PV = ('heart-surgery', 'pre-enforcement', 'N/A', 'role-based purpose enforcement') expresses that any request with the purpose of 'heart-surgery' should be pre-enforced by using the 'role-based enforcement' mechanism. For more detail on purpose enforcement information model, one can refer to Section 5.

To support this enforcement structure, we propose the enforcement model as presented in next section.

4 Purpose enforcement model for usage control

In this section, we present in detail the purpose-based usage enforcement model applied in distributed healthcare information system. The enforcement model focuses on the system architecture and functional modules to illustrate how the enforcement can be achieved.

As illustrated in Figure 2, the model consists of many components; we divide it into four main parts: the main components for usage control enforcement and modules for pre-, ongoing-, and post-enforcement. We present them in detail as following.

4.1 Main usage enforcement module

This module consists of three main components: Enforcement Point (EP), Decision Point (DP), and Session Management Point.

1 EP handles the request from the subject and forwards it to purpose validation point (for pre-enforcement) and then to decision point through session management point for further policy evaluation. If the usage request is granted by DP, then EP allows the subject to use resource, else, a denied message is sent to subject.

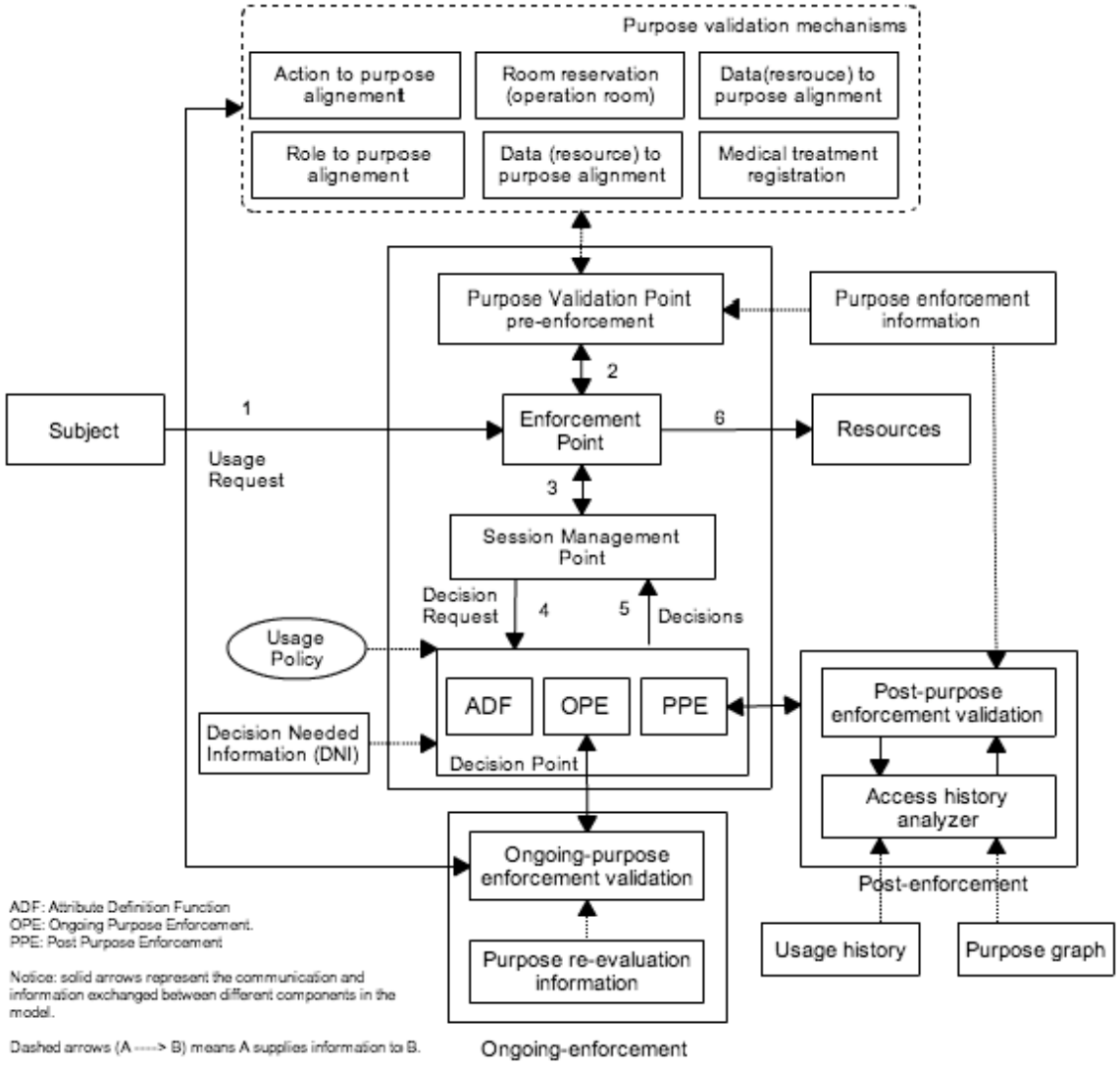
2 SMP manages individual usage session. This includes requesting required decision(s) from concerning modules (ADF, OPE and PPE) in each state during the usage session. When usage request is received, EP forwards it to SMP. SMP sends corresponding decision requests to DP. Then DP launches a checking process for all the concerned modules such as ADF, OPE, and PPE. If all the requirements are fulfilled, DP sends

granting message to SMP. Then, SMP forwards it to EP. In case of negative decision, SMP sends a denied response to EP. In the using state, the SMP monitors continuously related subject, object and environment attributes; as well as any further actions requested by the subject. According to the decision received from DP, SMP either revokes the ongoing usage by sending a revoked response to EP or keeps permitting access.

3 DP is responsible for making the permission decisions during usage control session based on usage policy. It consists of three decision-making components.

- Attribute Decision Function (ADF) handles the attribute-based access decision during usage session. Attributes can be either subject, object, or environment attributes (e.g. the subject's identification). The Information required by ADF is retrieved from DNI.
- Ongoing Purpose Enforcement (OPE) handles the re-evaluation of purpose during the usage of data. If the purpose is no longer valid, it informs DP to invoke the right and DP sends the order to end usage session to SMP.
- Post Purpose Enforcement (PPE) handles the evaluation of purpose in case pre- and ongoing-enforcements are not possible. The decision of this module is based on the usage history and purpose graph (the graph showing the relationship between purposes). If after data usage, the PPE finds that user violates the usage policy, the right to use data is revoked and the future usage is prohibited. It is important to note that the post-enforcement can be performed instantly after the usage of data or after a given period depending on the usage purpose enforcement information.

Figure 2 Purpose-based usage control enforcement model. User and subject are interchangeable, it refers to those who request to use data



4.2 Pre-enforcement module

Pre-enforcement module is responsible for validating the claimed purpose before granting access to user. This module consists of a purpose validation point connected to purpose validation mechanism and purpose enforcement information module.

1 Purpose Validation Point (PVP) makes the decision whether a purpose is valid or not. Whenever there is a request, PVP checks the request based on the claimed purpose. To validate the usage purpose, PVP contacts the purpose validation mechanism (Figure 2).

2 Purpose validation mechanism is responsible for validating the purpose of usage by using different validation mechanisms. The mechanisms used depend on type of purpose. Below are some examples of purpose validation mechanism. We divided the mechanisms into two types: general mechanisms that can be used not only for healthcare domain, but also for other domain-specific mechanisms that are designed for only healthcare system.

General mechanisms

- 'Role to purpose alignment' provides the information concerning the alignment between the user's role and the purpose of usage. For example, a user in role of 'cardiologist' may be aligned to the 'heart surgery purpose'. This information can be used for the pre-enforcement of purpose. However, using the role to purpose alignment alone may not be an effective solution to the problem as roles and purposes are not always aligned. Thus, this information needs to be used in conjunction with other information from other modules presented below.
- 'Action to purpose alignment' provides the information concerning the alignment between the actions on object and the purpose. However, like 'role to purpose', 'action to purpose' can be used only as the complement to other modules for purpose enforcement.
- 'Data to purpose alignment' provides the information concerning the alignment between type of object (resource or data) and purpose. For example, data concerning surgery may be aligned to the request for 'surgery purpose'.
- 'Consent/authorisation' provides the information about who is particularly authorised for which purposes. This module is administrated by the trusted entity that has the authority to align a particular user or a group of users to the particular purposes.

Specific mechanisms

- 'Medical treatment registration', in general, patient needs to register for the medical check. The registration information can be used to prove if the purpose claimed by the user is inline with the treatment of the patient. For instance, if the patient registered for general normal medical check, the users (e.g. doctor or physician) claimed purpose as 'emergency' is not valid.
- 'Room reservation (operation room or emergency room)' provides the information concerning the room reservation for each operation. This module is designed as the source of information in case of emergency situation. For example, in case of emergency situation, the usage rule on data may be bypassed; hence, operation room reservation can be the source of information to validate the claimed-purpose.

3 Purpose enforcement information (or purpose validation policy) provides the necessary information like, how the purpose should be validated with which mechanisms and at which phase of data usage, to remote client. This information is different from purpose to purpose. It is worth noting that the purpose enforcement information can be embedded in usage policy or can be expressed in a separate file.

4.3 Ongoing-enforcement module

This module is responsible for re-validating claimed purpose during usage session. It consists of the following components.

1 Ongoing purpose validation point is responsible for re-validating the purpose during the usage of data. With the information provided by purpose re-evaluation information module. It triggers the re-validation process periodically during the usage of data. If the claimed purpose is no longer valid given the change of time (or state) or other causes, this module informs DP to revoke the right and it ends the usage session. This module is also connected to purpose validation mechanisms. It is worth noting that both pre-enforcement and ongoing-enforcement may use the same validation mechanisms. The only difference is the phase at which the enforcement takes place.

2 Purpose re-evaluation information module provides the information concerning when the ongoing-enforcement should take place and what are the validation mechanisms we should use.

4.4 Post-enforcement module

This module handles the evaluation of purpose after the usage of data. The decision of this module is based on the auditing result of the past usage activities against the usage policy and the relation of the claimed purpose with other purposes that have been granted in the past. In this paper, we do not go into the details of methods used to audit the usage of data; we leave it for the future work.

1 Post purpose enforcement validation performs the validation of purpose after the usage of data. It communicates with the access history analyser to perform the analysing task of the past usage activities.

2 Access history analyser performs the auditing process on the usage history for a particularly data and its associate claimed purpose. If there is no violation of the usage policy, the positive response is sent to the post purpose enforcement point otherwise the negative response is sent.

3 Usage history provides the selected information in database. The selected information means only the information relevant to the claimed purpose and target data that system is auditing.

4 Purpose graph is a graph showing the inter-relationship between purposes. It is also called purpose tree. The intuition behind the use of purpose graph is that during the auditing process, we do not only examine the information related to claimed purpose, but also the information related to other purposes that have relationship with claimed purpose. This is because in some situation before achieving the claimed purpose, user may have to pass the intermediate states relating to other purposes and they have relationship with claimed purpose. With this information we can get to know the exact status of data processing and can make a knowledgeable decision. For more detail on how the purpose and purpose graph are modelled, one can refer to Rath and Colin (2013b).

4.5 Information flow of the model

This section presents a brief description of the data flow for the proposed model which is shown in Figure 2. It provides the overview of the communication between different components of the model.

- (1) Subject sends 'usage request' to EP where the purpose of usage is mentioned.
- (2) Upon receiving the usage request, EP retrieves the purpose of usage and sends the request to purpose validation point (pre-enforcement). If the purpose is valid, go to '(3)', otherwise, the process is ended here (at EP) and the negative response is sent to subject.
- (3) EP forwards the request to SMP.
- (4) SMP sends the decision request to DP where the usage policy is evaluated.
- (5) DP sends the decisions to SMP either positive or negative. If it is positive, the session starts. If it is negative, SMP simply forwards the decision to EP without starting the session.
- (6) Upon receiving the positive response, EP allows user to use requested resource.

Figure 3 Functioning of enforcement system (positive response), pre-enforcement

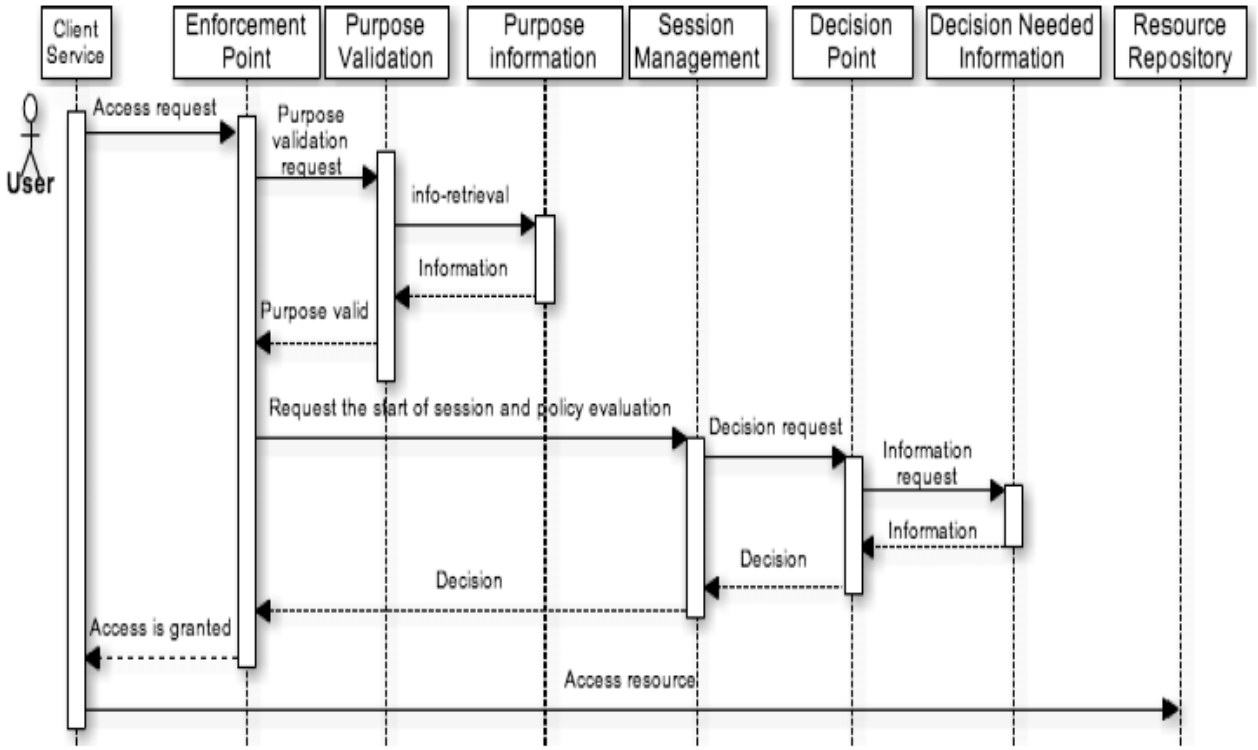
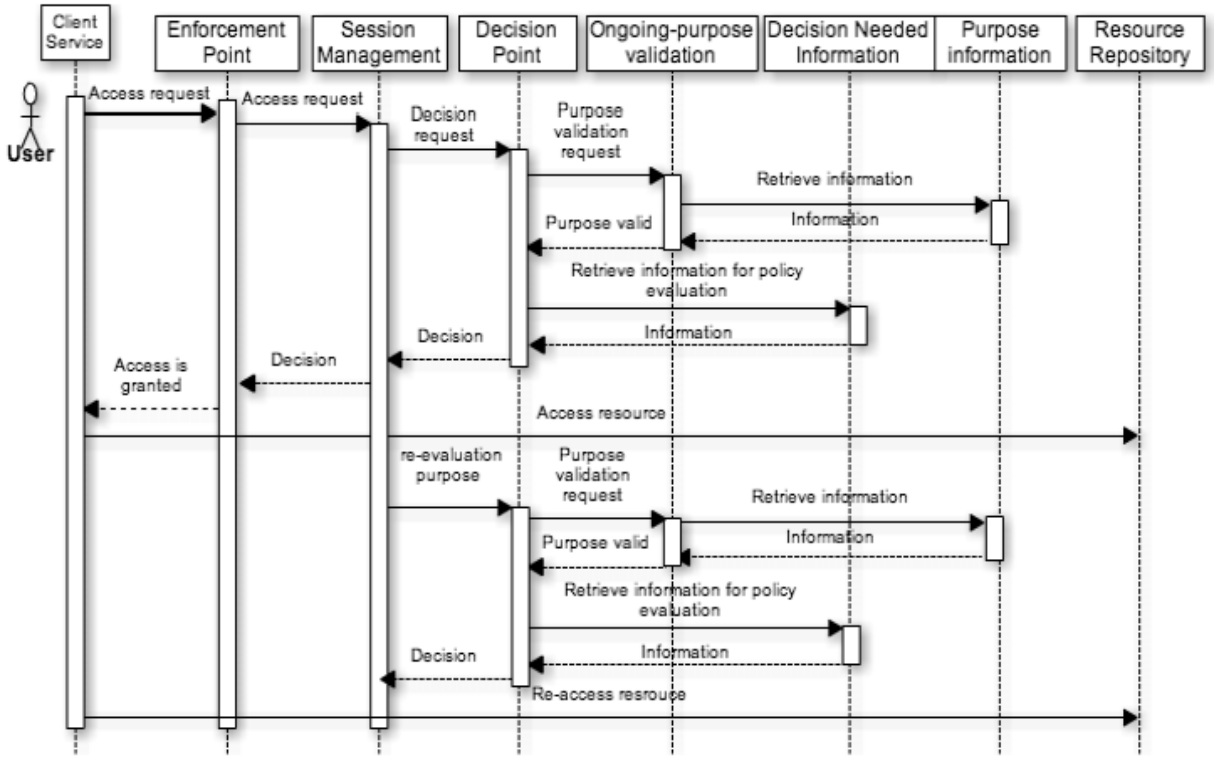


Figure 4 Functioning of enforcement system (positive response), ongoing-enforcement. Solid arrows represent the requests and dashed arrows represent responses



5 Model implementation

We designed a concrete usage control enforcement engine as presented in Figure 5. We then developed and tested a validation prototype in Java program. Furthermore, in order to utilise the existing standards and frameworks in the area of usage control, a modified XACML (enterprise-java-xacml, OASIS, 2013) Enterprise Java XACML is an implement of OASIS XACML 2.0 and intends to provide a high performance and good usability that can be used in enterprise environment, is used in this prototype as a core policy evaluation engine. Given that the usage enforcement should be done in a remote client platform, we have no control over the remote system. That requires trust establishment between the service provider and the remote client before any data are released. While the trust issue goes beyond the scope of this paper, we assume that the remote client is trusted before the usage control policy enforcement takes place.

5.1 XACML (Extensible Access Control Markup Language)

XACML is an OASIS standard that describes both the policy language and access control decision and response language. The policy language is, XML-based, used to describe the general access control requirements, while the access control decision request/response language aims at providing the means to form a query to ask whether or not a given action should be allowed or denied. The XACML policy language consists of three mains components: policy set, policy and rule.

- Policy set contains the target, rule-combining algorithm, obligation and advice. Target specifies the set of requests to which it applies, it is generally declared by the policy writer. Rule-combining algorithm specifies the procedure by which the results of evaluating the policy are combined when evaluating the policy. Obligation specifies the obligation that user or system needs to perform before granting access to user.
- Policy consists of the same components and they have the same functionality as that of policy set. Those components are target, rule-combining algorithm, obligation, and advice.
- Rule consists of rule target, condition, obligation and advice. ‘Condition’ represents a Boolean expression that refines the applicability of the rule beyond the predicates implied by its target. Therefore, it may be absent. The condition attributes can be defined by the rule-writer. ‘Advice’ may be added by the writer of the rule. When a PDP evaluates a rule containing advice expression, it evaluates the advice expressions into advice and returns certain of those advices to the PEP in the response context. Advice and obligation are different. Advice may be safely ignored by the PEP, while obligation is all time-compulsory task that needs to be executed by PEP. For more detail information, one can find it in XACML specification (OASIS, 2013).

5.2 Prototype

We prototype a remote client application for distributed healthcare system. This client application can control and

manage the usage of health record in accordance with the usage policy and the purpose enforcement information provided by source server. In our e-health scenario, the doctor requests patient's health record from the Healthcare Information System (HIS). After authenticating and authorising the doctor based on his/her role and purpose of usage, HIS releases the record, usage policy, and purpose enforcement information in one package. The package can reside on doctor device for a specific period of time during which doctor can re-access/re-use it. The enforcement component, which is integrated into the document reader (at client side), checks the integrity of the package and extracts the usage control policy, purpose enforcement information and patient's record. With those information, remote client application can control and manage the usage of record accordingly. Figure 5 shows the architecture of our usage control enforcement engine.

- PEP acts as single entry point to protected resources. It performs usage control. It receives the usage requests from requester, and first makes a Purpose Validation Request (PVQ) and consequently receives the response (PVR) from PVP. After receiving the positive response from PVP, it makes a usage decision request (DQ) to PDP 1 and PDP 2 through SMP and gets the decision response (DR) either positive or negative. Then SMP forwards the response to PEP. PEP enforces the authorisation decisions it receives by either allowing access or denying it.
- PVP acts as a validation point for purpose, which needs to be verified before further validation of the usage policy by PDP 1 and PDP 2. If PVP provides a negative response, the process ends and no further evaluation of usage policy. In case of positive response from PVP, a further decision request is sent to PDP 1 and PDP 2 through SMP for further usage policy evaluation.
- DP manages the decisions received from different decision modules such as: PDP1, PDP2 and PDP3. It then makes a final decision based on a specific algorithm.
- Purpose enforcement information provides all the necessary information to PVP during the validation state. The information provided to PVP comes from different modules (Figure 2). Those modules are responsible for providing information for different types of purpose. For example, in case of emergency heart surgery purpose, the role to purpose alignment and medical treatment registration modules are the sources of information.
- SMP is the dynamic part of the whole engine and captures the continuity behaviour of the usage control system. Furthermore, it manages the functions of other elements of the architecture and ensures the transitions from one to another state.
- Event handler handles the events that trigger transitions from one state to another. It listens to the events and sends the trigger actions to SMP when state change is about to occur.
- Timer can be set by the SMP through the event handler. Timer can be used for supporting re-evaluation process.
- PVM is the purpose validation mechanism that is used to evaluate the authenticity of the claimed purpose. This module is used by two modules: PDP2 for ongoing-enforcement and PVP for pre-enforcement.
- PDP 1 refers to ADF function in our enforcement model and it is represented as a XACML PDP. It is the component that evaluates attribute-related constraints (authorisations and conditions) and renders decisions to SMP.
- PDP 2 refers to OPE module of our enforcement model. It receives a re-evaluation request from the SMP and checks the re-evaluation rule from purpose 're-evaluation information'. It also renders decision to SMP.

5.3 Design of purpose validation point for pre-enforcement (PVP)

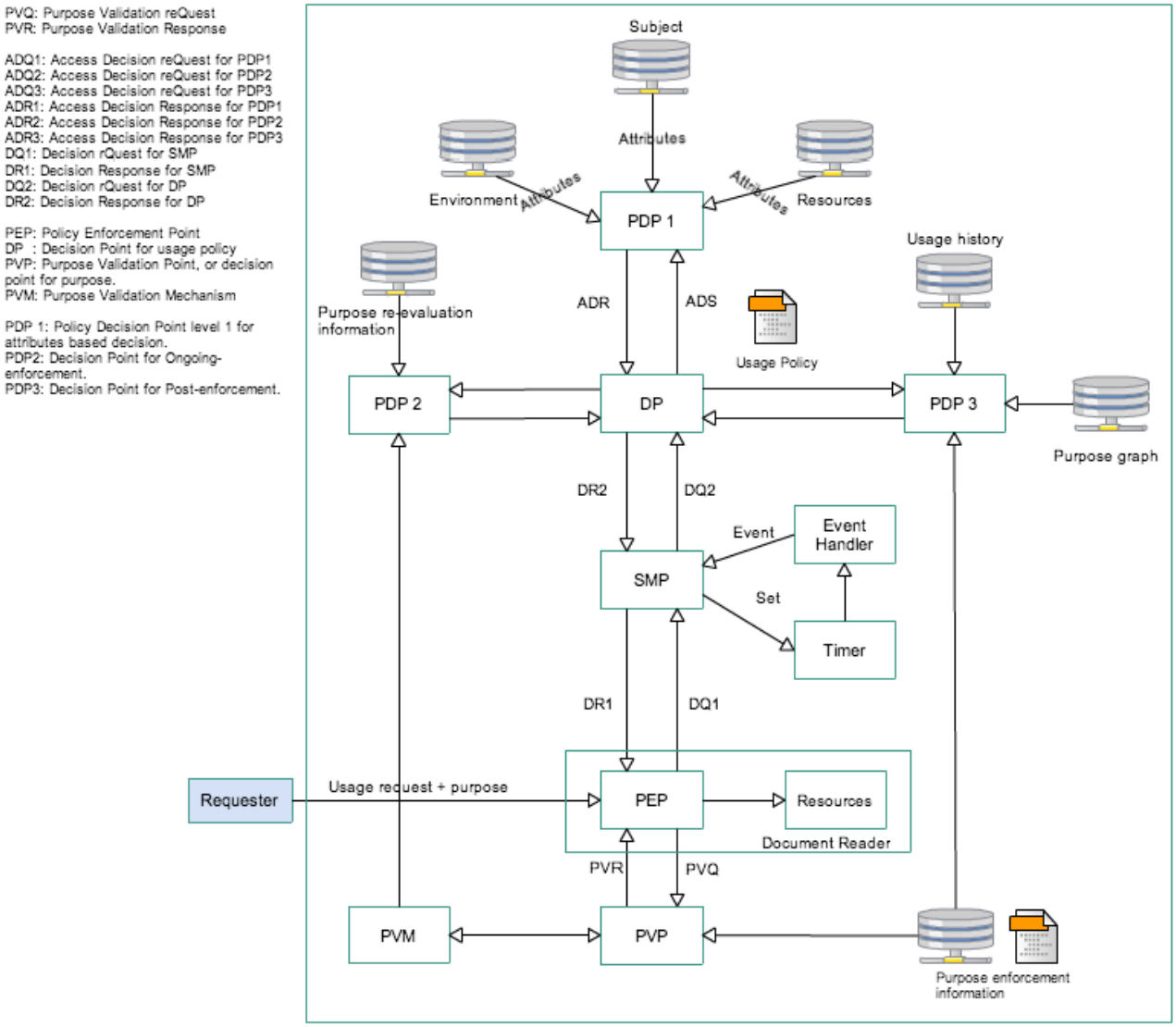
Based on our proposed model, the pre-enforcement of claimed purpose needs to be performed by the system before the usage session starts. We build a Java package to represent it and integrate into the XACML policy engine. This module receives the claimed purpose from PEP and contacts the purpose validation mechanism for further validation process. The six validation mechanisms (Figure 2) are implemented as Java packages where the information concerning the alignment between purpose and role, purpose and data, etc., is expressed in XML file.

PVP module provides two types of response: 'Valid' or 'Invalid'. They are expressed in XML file. 'Valid' means 'claimed purpose' is valid and PEP can forward the request to SMP for further policy evaluation while 'Invalid' means otherwise. It is worth noting that with 'Invalid', the processing of request is ended immediately by PEP and no further evaluation of usage policy by DP.

5.4 Design of ongoing purpose enforcement module

We built two Java packages to represent OPE module, one called 'Event Listener' is responsible for listening to the request from SMP where the event handler is attached. Whenever, it receives the signal for re-evaluation of purpose, it triggers the re-evaluation module, which is the second Java package. Then the re-evaluation module contacts the purpose re-enforcement information for necessary information concerning the re-evaluation before contacting the purpose validation mechanism module to validate purpose. OPE module has also two possible responses, 'Valid' and 'Invalid'. 'Valid' means 'claimed purpose' is still valid and the usage of data can be continued as it is; while 'Invalid' means 'claimed purpose' is no longer valid. Thus, the system needs to interrupt the usage of data. The interruption is done by DP, after receiving the negative response from OPE, DP sends 'permission deny' to SMP and then SMP sends an alert message 'ending usage session' to PEP. Finally, PEP alerts the user about the decision.

Figure 5 Implementation architecture. Arrows represents the requests and responses between components in the system (see online version for colours)



5.5 Design of the request structure

The request structure is composed of the following components: (U, R, A, O, P) where

1 'U' is a user who requests for data usage. It can be identified by user's name or identity.

2 'R' is a role of user in a particular institution. For example, cardiologist can be considered as user role. It is worth noting that in our implementation, we assume that user to role assignment is done by other modules and we do not address it here.

3 'A' is a requested action performing on resource or object. For example, transfer, copy, or read.

4 'O' is a targeted object by requester.

5 'P' is a claimed purpose, this is an important element in the request, user must declare their access purpose when initiating request.

It is also worth noting that we adopt the XACML's request structure in our implementation where the purpose of access is encoded in the environment attribute specified in standard XACML request.

5.6 Design of purpose validation information

Purpose validation information is the information provided to remote client application so that it can be used in purpose enforcement process. Those information are: 'the purpose of access', 'validation phase', 'validation mechanism' and 'time'. In our implementation, we express these information in xml file with the structure as presented in Figure 6. It is important to note that this structure is for the purpose of testing our model, it is not necessary a compete structure.

5.7 Implementation and testing

We built five components that form a usage control application. The first component is the document reader that

is responsible for processing the requested resource in the secure way. It also represents the PEP module. The second component is PVP. It is connected to the purpose validation mechanism. In our implementation, the six components of the purpose information point (role to purpose alignment, … refer to Figure 2) are encoded in XML format.

Figure 6 Example of XML-based structure of purpose validation information (see online version for colours)

```
<pv:purposevalidation >
        <pv:purpose>
                <pv:validationmechanism />
                <pv:enforcementphase />
                <pv:time />
        </pv:purpose>
</pv:purpose-validation>
```

The third component is the event handler, we use Java timer to set a time for triggering the event during the usage session. It is worth noting that 'Timer' acts upon the information from purpose enforcement information. The fourth component is the DP containing ADF and OPE. ADF module is based on the enterprise-java-xacml used for usage policy evaluation while OPE is for ongoing-enforcement.

To test our application, we created different types of policies. Some require only pre-enforcement and some require both pre- and ongoing-enforcement. The purpose of usage is classified into two types: normal and emergency. In a normal case, pre-enforcement is required and all the six purpose validation modules (Figure 2, ranging from 'action to purpose alignment' to 'medical treatment registration', most importantly 'consent/authorisation') need to be checked. In emergency case, pre-enforcement is ignored while ongoing-enforcement and post-enforcement are required. It is worth noting that we use the emergency scenario because we want to show the important of the 'post-enforcement of purpose'. In general, 'emergency usage' is a special case where the pre-enforcement of purpose may not be possible because system may allow user to use data although they are not entitle to use it. This is because we need to balance between the risk of patient's life and the safety of health record.

6 Discussion and future work

We proposed a general model for purpose enforcement applied for usage control in distributed healthcare. The model covers all the necessary functionalities for enforcing purpose of usage in different phases during the data usage lifecycle. If we go into the details of the model, we see clearly that the security of data depends largely on the effectiveness of the purpose validation mechanism. How to design a very effective validation mechanism that can be used for all types of purpose is still a question. This is because, in most cases, it is hard to verify if the purpose of usage can be achieved or not with a 100% sure decision as some purposes can be validated only either instantly or a while after the data usage. For example, 'accessing patient's record for the purpose of research', how to ensure that user uses those records for research, only after a certain period of time, we can conclude whether user has used those records for research purpose or not. Thus, the need of probabilistic approach. Our future research is to work on a type of purpose engine that is able to predict the future achievement of claimed purpose based on the historical usage activities of user, contextual knowledge related to claimed purpose, and relationship between claimed purpose and other purposes. This approach will leverage the security and make a more reliable purpose enforcement engine.

7 Conclusion

In this paper, we addressed the issue of purpose enforcement in usage control, applied to e-health domain as an illustration. We proposed a classification for enforcement mechanisms, based on the moment that happen in the usage timeline and defined pre-, ongoing-, and post-enforcement. Building on this classification, we proposed an original model for purpose enforcement, as well as a system architecture that introduced some generic components that contribute to the enforcement of usage purpose. A prototype of the model has been developed as a first step into validation. In this paper, we only dealt with the pre- and ongoing-enforcement cases while post-enforcement is left for the future work.

References

Alexander, P., Hilty, M. and Basin, D. (2006) 'Distributed usage control', *The ACM Communication,* pp.39–44.

Alexander, P., Manuel, H., Florian, S., Christian, S. and Thomas, W. (2008) 'Usage control enforcement: present and future', *IEEE Security and Privacy,* Los Alamitos, CA, USA.

Byun, J-W., Bertino, E. and Li, N. (2005) 'Purpose based access control of complex data for privacy protection', *Proceedings of the 10th ACM Symposium on Access Control Models and Technologies, SACMAT 05*, ACM, New York, USA.

Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R. and Chandramouli, R. (2001) 'Proposed NIST standard for role-based access control', *ACM Transactions on Information and System Security,* Vol. 4, Vol. 3, pp.222–274.

Jafari, M., Fong, P.W.L., Safavi-Naini, R., Barker, K. and Sheppard, N.P. (2011). 'Towards defining semantic foundations for purpose-based privacy policies', *Proceedings of the 1st ACM Conference on Data and Application Security and Privacy, CODASPY 11,* ACM, San Antonio, TX, USA, pp.213–224.

Jafari, M., Safavi-Naini, R-H. and Sheppard, N.P. (2009) 'Enforcing purpose of use via workflows', *Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society, WPES'09*, ACM, New York, NY, USA, pp.113–116.

Jawad, M., Alvarado, P.S. and Valduriez, P. (2008a) 'Formalizing and enforcing purpose restrictions in privacy policies', *Proceedings of the ACM 2008 International Workshop on Privacy and Anonymity in Information Society,* New York, USA.

Jawad, M., Alvarado, P.S. and Valduriez. P. (2008b) 'Design of PriServ, a privacy service for DHTS', *Proceedings of the 2008 International Workshop on Privacy and Anonymity in Information Society, PAIS'08*, ACM, New York, NY, USA, pp.21–25.

Katt, B., Zhang, X., Breu, R., Hafner, M. and Seifert, J-P. (2008) 'A general obligation model and continuity enhanced policy enforcement engine for usage control', *Proceedings of the 13th ACM symposium on Access control models and technologies (New York, NY, USA, 2008), SACMAT'08*, ACM, pp.123–132.

Li, W. and Hoang, D. (2009) 'A new security scheme for e-health system', *Proceedings of the International Symposium on Collaborative Technologies and Systems,* Washington, DC, USA, pp.361–266.

Lillian, R. (2008) 'An initial model and a discussion of access control in patient controlled health records', *Proceedings of the 3rd International Conference on Availability, Reliability and Security*, pp.935–942.

Ni, Q., Bertino, E., Lobo, J., Brodie, C., Clare-Marie, K. and Trombeta, A. (2010) 'Privacy-aware role-based access control', *ACM Transaction Information and System Security,* Vol. 13, No. 3, ACM, New York, USA.

OASIS (2013) *enterprise-java-xacml*. Available online at: http://code.google.com/p/enterprise-java-xacml/, http://docs. oasis-open.org/xacml/3.0/ xacml-3.0-core-spec-cs-01-en.pdf

Park, J. and Sandhu, R. (2002) 'Towards usage control models: beyond traditional access control', *Proceedings of the 7th ACM Symposium on Access Control Models and Technologies,* SACMAT 02, ACM, New York, NY, USA, pp.57–64.

Rath, A.T. and Colin, J-N. (2012a) 'Patient privacy preservation: P-RBAC vs OrBAC in patient controlled records type of centralized healthcare information system, case study of Walloon healthcare network, Belgium', *The 4th International Conference on eHealth, Telemedicine, and Social Medicine, eTELEMED 2012*, Spain, Valentia, Vol. 4, pp.111–118.

Rath, A.T. and Colin, J-N. (2012b) 'Analogue attacks in e-health: Issues and solutions', *CeHPSA – 2012: 2nd IEEE International Workshop on Consumer eHealth Platforms, Services and Applications (CeHPSA),* Las Vegas, USA.

Rath, A.T. and Colin, J-N. (2013a) 'Access and usage control requirements for patient controlled records type of healthcare information system', *The 7th International Conference on Health Informatics, HEALTHINF 2013*, Barcelone, Spain.

Rath, A.T. and Colin, J-N. (2013b) 'A purpose model and policy enforcement engine for usage control in distributed healthcare information system', *The 7th International Conference on Health Informatics, HEALTHINF 2013*, Barcelone, Spain.

Rengamani, H., Upadhyaya, S., Rao, H.R. and Kumaraguru, P. (2010). 'Protecting senior citizens from cyber security attacks in the e-health scenario: an international perspective', *ACM Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research,* New York, USA, 2010.

Russello, G., Dong, C. and Dulay, N. (2008) 'Consent-based workflows for healthcare management', *IEEE International Workshop on Policies for Distributed Systems and Networks,* pp.153–161, Los Alamitos, CA, USA.

Yarmand, M.H., Sartipi, K. and Down, D.G. (2008) 'Behavior-based access control for distributed healthcare environment', *IEEE Symposium on Computer-Based Medical Systems,* Los Alamitos, CA, USA, pp.126–131.

Zhang, X., Parisi-Presicce, F., Sandhu, R. and Park, J. (2005) 'Formal model and policy specification of usage control', *ACM Transaction on Information and System Security,* Vol. 8, No. 4, pp.351–387.